

Week 2- Identity and Access Management(IAM)

Name- Samruddhi Dattu Nikam

PRN-2124UCSF2019

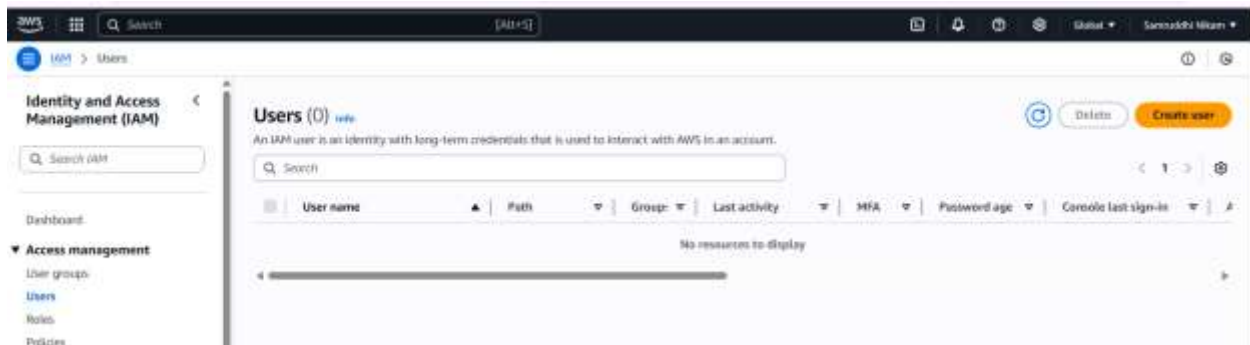
College Name- Sanjivani University

Email-Id- samruddhi.nikam_24ucs@sanjivani.edu.in

- ❖ Task- 1) Create IAM users, groups, roles.
- 2) Apply least privilege principle.
- 3) Document policies and screenshots.

🚦 Steps Create IAM users, Groups, Roles.

1. Sign in to AWS Console, Go to: <https://aws.amazon.com/> , Sign in using your root user or IAM user.
2. Create IAM User, Go to IAM → Users → Click on Create user.



3. Enter the User name, Select AWS Management Console access, then check custom password and reset the password and click Next Button.

Specify user details

User details

User name
Samruddhi

☒ Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in AWS Identity Center.

Are you providing console access to a person?

User type

☐ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to your AWS account and third applications.

☒ I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, session-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Week 2- Identity and Access Management(IAM)

Console password

☐ Autogenerated password
You can view the password after you create the user.

☒ Custom password
Enter a custom password for the user:

Must be at least 8 characters long
Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols: ! @ # \$ % ^ & * () _ + = { } [] ' "

☐ Show password

☒ Users must create a new password at next sign-in - Recommended
Users automatically get the `IAMUserChangePassword` policy to allow them to change their own password.

1 If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Activate Windows [Cancel](#) [Next](#)
Go to Settings to activate Windows.

4. Set the permission and then click the create group.

Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

☒ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

☐ Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

1 **Get started with groups**
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#) [Create group](#)

► **Set permissions boundary - optional**

[Cancel](#) [Previous](#) [Next](#)

5. Enter User group name, select the Permissions policies, and then click the create user group.

Create user group

Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

User group name
Enter a meaningful name to identify this group.
LimitedAccessGroup
Maximum: 128 characters. Use alphanumeric and '-', '_', and '.' characters.

Permissions policies (1/1050) [Create policy](#)

Filter by Type: All types 1 match

Policy name	Type	Used	Description
<input checked="" type="checkbox"/> AmazonEC2ReadOnlyAccess	AWS managed	None	Provides read-only access to Amazon EC2 resources.

[Cancel](#) [Create user group](#)

Week 2- Identity and Access Management(IAM)

6. Click Create user button.

The screenshot shows the AWS IAM 'Create user' console. A green banner at the top states 'LimitedAccessGroup user group created.' Below this, a progress bar indicates the current step is 'Review and create'. The 'User details' section shows 'User name: Samrudthink', 'Console password type: Custom password', and 'Require password reset: Yes'. The 'Permissions summary' table lists one policy: 'IAMUserChangePassword' (AWS managed, Permissions policy). The 'Tags' section is empty with an 'Add new tag' button. At the bottom right, there are 'Cancel', 'Permissions', and 'Create user' buttons.

7. User Created Successfully.

The screenshot shows the AWS IAM 'Retrieve password' console. A green banner at the top states 'User created successfully' with a 'View user' button. Below this, a progress bar indicates the current step is 'Retrieve password'. The 'Console sign-in details' section shows the 'Console sign-in URL' as 'https://555455852359.signin.aws.amazon.com/console', 'User name' as 'Samrudthink', and 'Console password' as 'XXXXXXXXXXXX' with a 'Show' button. At the bottom right, there are 'Cancel', 'Download .csv file', and 'Return to users list' buttons.

8. Create Role, click Role Option.

Dashboard

▼ Access management

User groups

Users

Roles

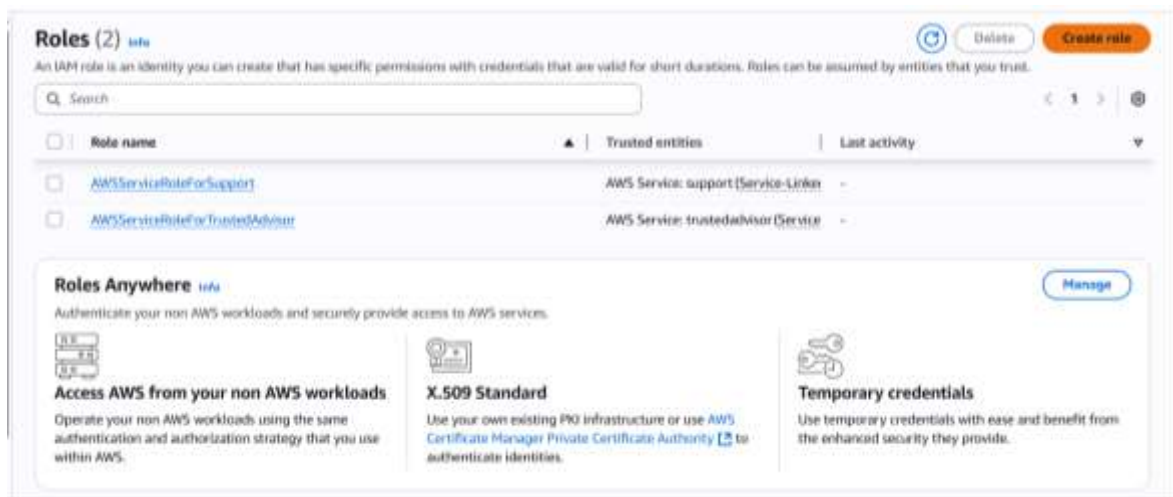
Policies

Identity providers

Account settings

Week 2- Identity and Access Management(IAM)

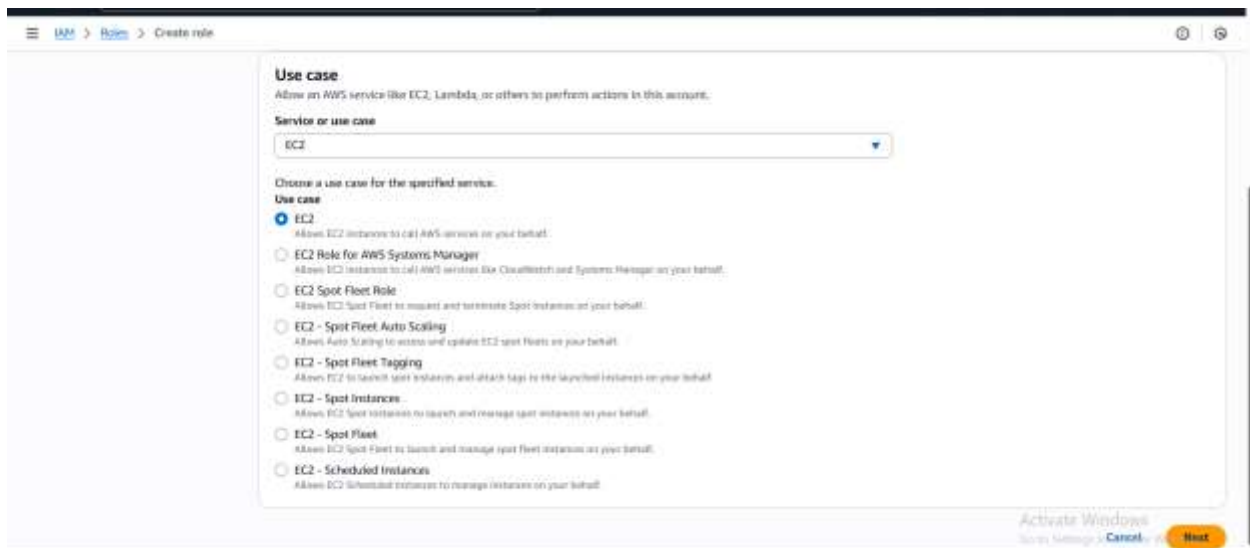
9. Click Create role.



10. Then select Trusted Entity.



11. Select the use case EC2, and then click Next.



Week 2- Identity and Access Management(IAM)

12. Attach the policies AmazonS3ReadOnlyAccess and CloudWatchAgentServerPolicy and click next Button.

The first screenshot shows the 'Add permissions' step in the AWS IAM console. The search bar contains 'amazonS3', and the filter is set to 'All types'. The results show 7 matches. The 'AmazonS3ReadOnlyAccess' policy is selected. The second screenshot shows the same step with the search bar containing 'cloudwatchagent' and the filter set to 'All types'. The results show 2 matches. The 'CloudWatchAgentServerPolicy' is selected.

Permissions policies (2/1050)

Choose one or more policies to attach to your new role.

Filter by Type: All types 7 matches

Policy name	Type	Description
<input type="checkbox"/> AmazonS3FullAccess	AWS managed	Provides full access to all buckets via t...
<input type="checkbox"/> AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	Provides AWS Lambda functions perm...
<input type="checkbox"/> AmazonS3OutpostsFullAccess	AWS managed	Provides full access to Amazon S3 on ...
<input type="checkbox"/> AmazonS3OutpostsReadOnlyAccess	AWS managed	Provides read only access to Amazon S...
<input checked="" type="checkbox"/> AmazonS3ReadOnlyAccess	AWS managed	Provides read only access to all bucket...
<input type="checkbox"/> AmazonS3TablesFullAccess	AWS managed	Provides full access to all S3 table bu...
<input type="checkbox"/> AmazonS3TablesReadOnlyAccess	AWS managed	Provides read only access to all S3 tabl...

► Set permissions boundary - optional

Activate Windows
Go to Settings to activate Windows.

Permissions policies (2/1050)

Choose one or more policies to attach to your new role.

Filter by Type: All types 2 matches

Policy name	Type	Description
<input type="checkbox"/> CloudWatchAgentAdminPolicy	AWS managed	Full permissions required to use Amaz...
<input checked="" type="checkbox"/> CloudWatchAgentServerPolicy	AWS managed	Permissions required to use AmazonCl...

► Set permissions boundary - optional

Cancel Previous Next

13. Give the Role details like name, Description.

The screenshot shows the 'Name, review, and create' step in the AWS IAM console. The role name is 'EC2BasicRole' and the description is 'Allow EC2 instances to call AWS services on your behalf.'

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and "+" characters.

Description
Add a short explanation for this role.

Maximum 2000 characters. Use letters (A-Z and a-z), numbers (0-9), hyphen, or any of the following characters: ., !, @, #, \$, %, ^, &, *, ~, `.

Week 2- Identity and Access Management(IAM)

14. Select Trusted Entities and check the permission.

Step 1: Select trusted entities Edit

Trust policy

```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Action": [
7-         "sts:AssumeRole"
8-       ],
9-       "Principal": {
10-        "Service": [
11-          "ec2.amazonaws.com"
12-        ]
13-      }
14-    ]
15-  }
16- }
```

Step 2: Add permissions Edit

Permissions policy summary

Policy name ↗	Type	Attached as
AmazonS3ReadOnlyAccess	AWS managed	Permissions policy
CloudWatchAgentServerPolicy	AWS managed	Permissions policy

15. Successfully Role is Created.



Week 2- Identity and Access Management(IAM)

✚ Apply least privilege principle.

LimitedAccessGroup info Delete

Summary Edit

User group name
LimitedAccessGroup

Creation time
June 15, 2025, 15:51 (UTC+05:30)

ARN
[arn:aws:iam::355433852359:group/LimitedAccessGroup](#)

Users

Permissions

Access Advisor

Permissions policies (1) info

You can attach up to 10 managed policies.

Filter by Type
All types

< 1 >

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AmazonEC2ReadOnlyAccess	AWS managed	1

Samruddhinik info Delete

Summary

ARN
[arn:aws:iam::355433852359:user/Samruddhinik](#)

Console access
[Enabled without MFA](#)

Access key 1
[Create access key](#)

Created
June 15, 2025, 15:33 (UTC+05:30)

Last console sign-in
[Never](#)

Permissions

Groups

Tags

Security credentials

Last Accessed

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type
All types

< 1 >

<input type="checkbox"/>	Policy name	Type	Attached via
<input type="checkbox"/>	IAMUserChangePassword	AWS managed	Directly

EC2BasicRole info Delete

Summary Edit

Creation date
June 15, 2025, 15:43 (UTC+05:30)

ARN
[arn:aws:iam::355433852359:role/EC2BasicRole](#)

Instance profile ARN
[arn:aws:iam::355433852359:instance-profile/EC2BasicRole](#)

Last activity

Maximum session duration
1 hour

Permissions

Trust relationships

Tags

Last Accessed

Revoke sessions

Permissions policies (2) info

You can attach up to 10 managed policies.

Filter by Type
All types

< 1 >

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS managed	1
<input type="checkbox"/>	CloudWatchAgentServerPolicy	AWS managed	1

Activate Windows
Go to Settings to activate Windows.